

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE U		PAGE 1		OF 3		PAGES	
2. AMENDMENT/MODIFICATION NUMBER P00002			3. EFFECTIVE DATE 12/05/2022		4. REQUISITION/PURCHASE REQUISITION NUMBER 1300904750-0002			5. PROJECT NUMBER (If applicable) N/A			
6. ISSUED BY NAVWAR-NIWC Atlantic (CHRL) P.O. BOX 190022 North Charleston, SC 29419-9022			CODE N65236		7. ADMINISTERED BY (If other than Item 6) DCMA Manassas 14501 George Carter Way, 2nd Floor Chantilly, VA 20151			CODE S2404A		SCD C	
8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code) Spinvi Consulting, LLC 12359 Sunrise Valley Dr Ste 120 Reston, Virginia 20191-3437						<input checked="" type="checkbox"/> (X)		9A. AMENDMENT OF SOLICITATION NUMBER			
						<input type="checkbox"/>		9B. DATED (SEE ITEM 11)			
						<input checked="" type="checkbox"/> (X)		10A. MODIFICATION OF CONTRACT/ORDER NUMBER N0017819D8560/N6523622F3043			
CODE 6LJ06						FACILITY CODE 055889488		10B. DATED (SEE ITEM 13) 09/26/2022			

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

SEE SECTION G

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.
IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.**

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
<input type="checkbox"/>	
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Mutual agreement with the parties IAW 52.232-33 and FAR 43.103(a)
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible)

SEE PAGE 2

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) (b) (4), (b) (6)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Sean Johnson , Contracting Officer	
15B. CONTRACTOR/OFFEROR (b) (4), (b) (6) (Signature of person authorized to sign)	15C. DATE SIGNED 12/05/2022	16B. UNITED STATES OF AMERICA /s/Sean Johnson (Signature of Contracting Officer)	16C. DATE SIGNED 12/05/2022

Previous edition unusable

General Information


PR 1300904750-0002

(b) (4)



This modification also includes travel updates to paragraph 11.1 located in Section C of the Performance Work Statement, and incorporating the finalized DD254.

(b) (4)



(b) (4)

ORDER FOR SUPPLIES OR SERVICES										PAGE 1 OF 99	
1. CONTRACT/PURCH ORDER/AGREEMENT NO. N0017819D8560			2. DELIVERY ORDER/CALL NO. N6523622F3043		3. DATE OF ORDER/CALL (YYYYMMDD) 2022DEC05		4. REQUISITION/PURCH REQUEST NO. 1300904750-0002		5. PRIORITY Unrated		
6. ISSUED BY NAVWAR-NIWC Atlantic (CHRL) P.O. BOX 190022 North Charleston, SC 29419-9022				7. ADMINISTERED BY (if other than 6) DCMA Manassas 14501 George Carter Way, 2nd Floor Chantilly, VA 20151		8. DELIVERY FOB SCD: C <input type="checkbox"/> DESTINATION <input type="checkbox"/> OTHER (See Schedule if other)					
9. CONTRACTOR NAME AND ADDRESS Spinvi Consulting, LLC 12359 Sunrise Valley Dr Ste 120 Reston, VA 20191-3437				10. DELIVER TO FOB POINT BY (Date) (YYYYMMDD) SEE SCHEDULE		11. X IF BUSINESS IS <input checked="" type="checkbox"/> SMALL <input type="checkbox"/> SMALL DISADVANTAGED <input type="checkbox"/> WOMEN-OWNED		12. DISCOUNT TERMS Net 30 Days WAWF			
				13. MAIL INVOICES TO THE ADDRESS IN BLOCK SEE SECTION G							
14. SHIP TO SEE SECTION F				15. PAYMENT WILL BE MADE BY DFAS Columbus Center, South Entitlement Operations P.O. Box 182264 Columbus, OH 43218-2264				MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.			
16. TYPE OF ORDER		DELIVERY/CALL <input checked="" type="checkbox"/>		This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.							
		PURCHASE <input type="checkbox"/>		Reference your _____ furnish the following on terms specified herein.							
ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.											
Spinvi Consulting, LLC NAME OF CONTRACTOR				(b) (4), (b) (6) SIGNATURE		(b) (4), (b) (6) TYPED NAME AND TITLE		DATE SIGNED (YYYYMMDD)			
<input type="checkbox"/> If this box is marked, supplier must sign Acceptance and return the following number of copies:											
17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE SEE SCHEDULE											
18. ITEM NO.		19. SCHEDULE OF SUPPLIES/SERVICES				20. QUANTITY ORDERED/ACCEPTED*		21. UNIT	22. UNIT PRICE	23. AMOUNT	
		SEE SCHEDULE									
*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.				24. UNITED STATES OF AMERICA /s/Sean Johnson BY:				12/05/2022 CONTRACTING/ORDERING OFFICER		25. TOTAL (b) (4)	
26. DIFFERENCES											
27a. QUANTITY IN COLUMN 20 HAS BEEN <input type="checkbox"/> INSPECTED <input type="checkbox"/> RECEIVED <input type="checkbox"/> ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:											
b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE					c. DATE (YYYYMMDD)		d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE				
e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE					28. SHIP. NO. <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		29. D.O. VOUCHER NO.		30. INITIALS		
f. TELEPHONE NUMBER		g. E-MAIL ADDRESS			31. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL		32. PAID BY		33. AMOUNT VERIFIED CORRECT FOR		
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.									34. CHECK NUMBER		
a. DATE (YYYYMMDD)		b. SIGNATURE AND TITLE OF CERTIFYING OFFICER							35. BILL OF LADING NO.		
37. RECEIVED AT		38. RECEIVED BY (Print)		39. DATE RECEIVED (YYYYMMDD)		40. TOTAL CONTAINERS		41. S/R ACCOUNT NUMBER		42. S/R VOUCHER NO.	

Section C - Description/Specifications/Statement of Work

SECTION C – DESCRIPTION/SPECS/WORK STATEMENT

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

SHORT TITLE: DEFENSE HEALTH INFRASTRUCTURE AND APPLICATION ENGINEERING

1.0 PURPOSE

1.1 SCOPE

Naval Information Warfare Center Atlantic (NIWC Atlantic) is responsible for providing Information Assurance, Network Infrastructure Operations Support, Engineering, and Program Management support, among other areas of interest, within the Department of Defense (DoD) medical community.

This PWS will provide worldwide enterprise Health Information Technology engineering support in the areas of system engineering, systems administration, enterprise network, network security, infrastructure engineering, infrastructure modernization, Information Technology (IT) systems, systems deployment and integration, information assurance and system support services. Support will be provided for entities that require connectivity and integration into the Medical Community of Interest (MedCOI) network that Navy Medicine and DHA own and operate; including DoD Medical departments (Air Force Medicine, Army Medicine, Navy Medicine), the Defense Health Agency (DHA), United States Coast Guard (USCG), the Veteran's Administration (VA), Defense Manpower Data Center (DMDC), Defense Healthcare Management System Modernization (DHMSM), and Defense Medical Information Exchange (DMIX) .

The tasking set forth below is intended to encompass the full operating lifecycle networks, network/application services and the health care applications they support. This support encompasses network protection from inception to operations network protection architecture, design, integration/deployment, and operation. Support for the network itself is not enough as the critical assets it is built to support are the health care applications and their supporting computing services, such as directory services. All of these items critically tie together for delivery of functional applications on a secure network.

NOTE: Website and e-mail addresses referenced within the PWS and Contract Data Requirements List (CDRL) forms are subject to change. For any website and e-mail address not working during time of performance, the contractor shall contact the Contracting Officer's Representative (COR) or Contracting Officer for latest website and e-mail address. An incorrect website or e-mail address does not alleviate a contractor from required reporting or access requirements.

1.1.1 Multiple Funding

This task order is funded with multiple appropriations as delineated on specified contract line item numbers (CLINs). The applicable PWS task(s) associated with each CLIN is outlined in Section B and Section G.

2.0 **PLACE(S) OF PERFORMANCE**

2.1 GOVERNMENT FACILITIES

Government facilities (i.e., office space or lab space) are provided to those contractor personnel that would otherwise adversely affect the work performance if they were not available on Government site. Labor categories with supplied Government facilities shall be located at:

- a. NIWC Atlantic, Charleston, SC
- b. NIWC Pacific, Pearl City, HI
- c. San Antonio, TX
- d. Washington, DC

2.1.1 Access to Government facilities

NIWC Atlantic and other Government installations have restricted access. Contractors are limited to access during certain days and times as specified in the workweek requirements of this PWS. If access to the assigned Government facility is restricted due to safety/security exercise, an Executive Order, or an administrative leave determination applying to the local activity (e.g., inclement weather), the contractor, in agreement with the COR, shall make alternative work arrangements. The contractor shall adjust work schedule, work at an alternate location, or if alternate work arrangements cannot be accommodated, the contractor shall notify the COR of the inability to access the assigned facility prior to charging their time to the task order as direct cost provided such charges are consistent with the contractor's accounting practices. The ability to work at an alternate location that is not a Government or contractor facility site is dependent on the contractor having an alternative work site agreement with the employee. The ability to work at an alternate location may not be an option for certain support services.

2.1.2 Training Requirements and Exercise Support

Contractor personnel working full-time or partially at a Government facility shall complete all applicable training requirements as specified under Mandatory Training, PWS Para 8.0. Contractor personnel may also be required to participate in safety, security (e.g., Anti-Terrorism Force Protection (AT/FP)), and operational training exercises (possibly two per year). Applicable contractor personnel shall support and participate in the training exercise which may include role-playing and reacting to exercise injects based on the situation or exercise objectives.

2.1.3 Emergency Management at Government Installations

During emergency situations including health (e.g., COVID-19 pandemic) and weather related circumstances, contractor personnel with scheduled access to a Government installation shall coordinate with the COR prior to reporting to their Government worksite. Access will be in accordance with the latest Government installation requirements and restrictions. The contractor shall identify with the COR if certain personnel are designated mission essential and determine the work expectations during the emergency period of performance. Depending on the type of support, working from an alternative worksite may or may not be allowed.

2.2 CONTRACTOR FACILITIES

A significant portion of work issued under this task order requires close liaison with the Government. The contractor shall establish a local facility within a fifteen (15)-mile radius of NIWC Atlantic, Charleston, SC. The contractor shall be capable of quickly interfacing with the labs located at NIWC Atlantic. The contractor's facility is not necessarily for the exclusive use of this task order and can be utilized on a shared basis. The contractor shall meet all facility location and size requirements within 30 days after task order award. The contractor shall ensure facility includes space for offices, conference rooms, lab work, and a staging area for materials and equipment. The contractor shall provide necessary unclassified space to support network protection development labs and integration center for single security architecture equipment suites. Additionally, the space will support network and cyber security operations center in support of the DHA enterprise networks in Charleston, SC.

Description	Part #	Unit/Issue	Quantity
Operations Space		Sq. ft	50,000 sq. ft.

2.3 ALTERNATE WORK LOCATIONS

The ability to provide support from an alternate location (includes working from an employee's residence or other non-Government facility) is dependent on the type of support required, the contractor employee's ability and trustworthiness, and the company's employment policy. Allowing work to be performed at an alternate location is not an option for all positions and personnel. The ultimate decision to allow work performed at an alternate work location will be determined by the COR. If alternate work locations are allowed, the company shall have defined criteria addressing the minimum requirement to have continuous, secure internet connectivity. Each applicable contractor employee shall have an established signed telework agreement between the company and employee. For each contractor employee proposed to work at an alternate location, the contractor shall submit a written request and justification to the COR with a copy of the applicable employee's signed telework agreement which becomes part of the COR files. If the requirements for teleworking and/or alternate work locations are not outlined/specified in the employee agreement documentation, the contractor shall include a copy of those requirements with the signed employee agreement. Working at an alternative location shall not adversely affect the response time required in support of the task order. The Government reserves the right to disallow any billable hours by contractor employees working at an alternative work location without obtaining prior Government approval. / The Government reserves the right to discontinue the ability to work from an alternate location at any time without cause. The inability of a contractor to respond to the requirements of the task order due to telework conditions will be negatively reflected in the Contractor Performance Assessment Reporting System (CPARS). The contractor shall utilize the Government site or Client site (vice contractor site) overhead labor rate for personnel working from their residence unless their Accounting System requires a different billing structure.

2.4 SPECIAL ACCESS LOCATIONS

Specific to orders requiring a Top Secret facility clearance with access to Sensitive Compartmented Information (SCI), the contractor shall provide support and resources that meet all security requirements for special access at the following locations:

NIWC Pacific, Pearl Harbor HI
USEUCOM, Stuttgart, GE
USAFIRCOM, Stuttgart, GE
The Pentagon, Washington, DC
USCYBERCOM, Ft. Meade, MD
DISA HQ, Ft. Meade, MD
Defense Health Agency, Falls Church, VA
DISA, Chambersburg, PA
FLTCYBERCOM, Ft. Meade, MD
NCDOC, Suffolk, VA
NSA, Ft. Meade, VA
DIA, Washington, DC
AFCYBER, San Antonio, TX
ARCYBER, Ft. Belvoir, VA
MARFORCYBER, Quantico, VA
USEUCOM, Molesworth, GB
NIWC Atlantic, New Orleans, LA
NAVIFOR, Norfolk, VA
NIWC Pacific, Honolulu, HI
NATO, Brussels, Belgium
USAG Daegu, South Korea
FLTCYBERCOM, San Diego, CA
CFA, Yokosuka, Japan

3.0 PERFORMANCE REQUIREMENTS

PR# 11731319	ESABAD Comply to Connect Support
PR# 11729212	ESABAD DMDC Dual Support
PR# 11731316	ESABAD Engineering Support HSSE IPT
PR# 11828390	DHMSM NIWC GAL NETOPS
PR# 11731318	MEDCOI LCDS Support
PR# 11802654	ESABAD MEDCOI Last Mile, SSA Deployment, Coordination, Network Ops Support-HSSE IPT
PR# 11795882	NetOps Support NIWC (HSSE IPT)
PR# 11780660	NIWC NetOps Support-HSSE IPT
PR# 11776159	ESABAD CG Netops ENG PMO support-HSSE IPT
PR# 11726071	ESABAD VA ES NSOC support-HSSE IPT
PR# 11829583	ESABAD VA Engineering & NSOC Support

The following paragraphs list non-personal services tasks that will be required throughout this task order. The contractor shall provide necessary resources with knowledge and experience as cited in the personnel qualification requirement to support the listed tasks. The contractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) that do not include performance of inherently Government functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

The contractor shall work closely with the government COR and when applicable provide support at the sponsor level.

3.1 GOVERNMENT CONTROLLED EQUIPMENT

In the performance of this work, the contractor shall use Government-provided Windows 10 computing platform image on all contractor-owned computer assets supporting this task order. Contractor personnel shall arrange with Government personnel for computer assets to be loaded with appropriate software. During the task order performance, the contractor shall track all computer assets with the Government-provided platform image and report in the monthly task order status report the quantities and location of each asset. In the event the asset is damaged/unfixable, no longer needed, or at the completion of the task order, the contractor shall arrange with the appropriate Government personnel for each asset to be cleaned/erased of all Government provided software and platform images. In the event a Government controlled asset is lost or stolen, the contractor shall notify the COR verbally and in writing no later than 24 hours from the time the asset is known missing.

3.2 PROGRAM MANAGEMENT SUPPORT

3.2.1 Program Support

The Contractor shall provide Project Management (PM) services for planning, organizing, and managing resources to bring about the successful execution of specific program/project goals and objectives as defined in this PWS. The primary objective of this task is to achieve all of the project goals and objectives, while adhering to specific project constraints (scope, quality, schedule and cost). The Contractor PM process shall ensure that the groundwork for the successful completion of all tasks is adequately established. Coordination of meetings, preparing budget drills, developing agenda items, attending high-level meetings, generating minutes, and tracking actions items may be required (CDRL A001).

The contractor PM shall apply standards, principles, and techniques of project management to monitor, control, and direct completion of all requirements, from receipt and initiation through planning, scheduling, execution, monitoring, transition, and closure. Project managers identify and facilitate activities required to complete projects reliably, on schedule, and within budget during the planning, design, engineering, test and evaluation, deployment, and transition phases of project life cycles.

3.2.2 Program Support Documentation

The contractor shall draft and/or develop various program management (PM) documents (CDRL A001). At a minimum, the contractor shall be required to draft and/or develop the following documents:

- Meeting Agenda and Minutes
- Plans of Action and Milestones
- Responding to data calls

3.2.3 Analysis of Alternatives (Planning, Alternatives Analysis, Reporting, Briefing)

The contractor shall conduct a thorough, detailed, and structured analysis of technical alternatives (AoA). The AoA approach shall include:

- A review of functional and technical requirements and specifications
- Development of detailed evaluation criteria (cost, benefit, functional, technical, schedule)
- Established scoring and weighting methodologies
- Development of an AoA Plan
- Conducting the structured analysis
- Generating a detailed report with recommendations, along with required technical and executive level briefings
- Coordination and obtaining key stakeholder buy-in to evaluation criteria, scoring methods, weighting, and the overall plan

The approach to be used shall include generation of draft and final deliverables for Government review and approval. Additionally, the approach shall include engagement with key stakeholders to ensure consensus with both the process, as well as the recommendations at the conclusion of the AoA. All documentation requests shall be delivered as Program Management Reports (CDRL A001).

3.2.4 Trade Studies (Technology Assessments and Insertion)

The contractor shall provide resources with a sound understanding of current technologies and technology trends; including systems hardware, software, systems architecture and design strategies, and key technologies of direct relevance and potential value to NIWC Atlantic customers.

Combined with market research and an understanding of customer requirements, the contractor shall employ a structured, AoA-type approach when conducting trade studies and trade-off analyses in support of technology assessments, technology refresh initiatives, and the insertion of key technologies into an enterprise to realize a return on investment (ROI). All documentation requests shall be delivered as Program Management Reports (CDRL A001).

3.3 INFRASTRUCTURE ARCHITECTURE DEVELOPMENT

3.3.1 Architecture, Design, and Senior Engineering Support

The contractor shall provide senior level enterprise architecture consulting services for programs supporting Defense Health customers. This support is essential to the establishment of the MedCOI network supporting the Military Health System (MHS) Genesis. These services shall include the development of DoD Architecture Framework (DODAF) artifacts which shall include:

- All Viewpoint (AV)
- Capability Viewpoint (CV)
- Data and Information Viewpoint (DIV)
- Operational Viewpoint (OV)
- Project Viewpoint (PV)
- Services Viewpoint (SvcV)
- Standard Viewpoint (StdV)
- Systems Viewpoint (SV)

The contractor shall provide network and network protection architectures that are compliant with all DoD Information Assurance (IA) requirements. The contractor shall support these designs/architectures through the DoD certification and accreditation process.

In addition to the development of network and network protection architectures, the contractor shall assist in the development of enterprise datacenter and server computing/service delivery (cloud computing) requirements documents and architecture designs. These requirements documents shall leverage industry best practices and the architecture designs must be compliant with all DoD IA requirements.

The contractor shall have subject matter expertise (SME) in engineering service projects. These service projects include ***but are not limited to:***

- Engineering cloud solutions in Amazon Web Services (AWS), Microsoft Azure, MilCloud, and Oracle
- Expanding the DHA Med-COI to external agencies to include Coast Guard, Veterans Administration, military reserves, etc.
- DHA IT Infrastructure refreshes

- DHMSM
- DHA Network Protection Suite (NPS) architecture design development and reviews
- Network device configuration and load testing
- Developing DoD Cloud access points in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS)

In support of the integration of DoD networks for the Electronic Health Record (EHR), the contractor shall leverage experience in each of these areas listed above to develop the documents below. All documentation requests shall be delivered as Technical Reports (CDRL A002).

- Requirements Documents
- Concepts of Operations (CONOPS)
- System specification and design documents
- System implementation plans
- System sustainment plans

3.3.2 IT Strategic Planning

The contractor shall provide support to senior strategic planning offices within DHA and DHMS. The contractor shall develop IT strategic plans that are mapped to organizational goals and objectives, and that track to capital planning and investment control (CPIC) processes for managing IT investment. This strategic and tactical planning approach shall be fully compliant with OMB guidelines and directives and shall also be linked into the overall, organizational EA and enterprise lifecycle management (ELM). All documentation requests shall be delivered as Technical Reports (CDRL A002).

3.4 ADVANCED INFRASTRUCTURE DESIGN AND TESTING

3.4.1 Network Protection Infrastructure Design Efforts

The contractor shall support network protection infrastructure design for large scale, global, enterprise networks supporting tens of thousands of users requiring protection of Protected Health Information and Personally Identifiable Information. The target network will also require protections necessary for a DoD Community of Interest (COI) network designed as a Mission Partner Enterprise (MPE) which is logically separated from the NIPRNet to allow interconnection of other Federal Government entities. The contractor shall apply a systems design approach to the directed efforts to ensure that the mission, objectives, and criteria requirements of specified systems are fulfilled. Emphasis shall be on the demonstration of clear, definable and auditable duplication of performance, logistics supportability, reliability, and maintainability of the item, subsystems, and systems. The contractor shall also provide demonstration that system designs include consideration for future scalability and adaptability of all item, subsystems, and systems. The contractor shall provide the following support and all documentation requests shall be delivered as Technical Reports (CDRL A002):

- Provide IA and network engineering support during requirements discussions and definition and contribute to required project meetings as necessary.

- Provide security requirements, design, installation and integration recommendations for network and other security systems as defined above.

3.4.2 Internet Protocol Version 6 (IPv6) Testing

The contractor shall assess each component submitted in a design, used in a lab environment or deployed for production use to determine IPv6 capability. The contractor shall follow the Government provided IPv6 Test Plan to determine IPv6 capability. The contractor shall also provide Commercial Off The Shelf (COTS) solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of Internet Protocol Version 4 (IPv4). Specific criteria to be deemed IPv6 capable are devices in Conformance to the DoD Information Technology Standards Repository (DISR) developed DoD IPv6 Standards Profile. Systems being developed, procured or acquired shall comply with the Global Information Grid Architecture and DISR standard IPv6 Capable definition. An IPv6 Capable system shall meet the IPv6 base requirements defined in the “DoD IPv6 Standards Profile v3.0” dated June 13, 2008. IPv6 traffic throughput and load testing shall be performed with the Government furnished BreakingPoint load tester. All documentation requests shall be delivered as Technical Reports (CDRL A002).

3.4.3 Product Evaluations

The contractor shall assess various network protection and infrastructure products against a set of criteria provided by the Government. This will include building candidate configurations, testing configurations to validate manufacturer performance and capabilities claims. Performance testing shall be conducted in the Government lab using the BreakingPoint load tester. At the completion of the testing, the contractor shall provide a report to the Government detailing the results of the testing and a recommendation for product selection. All documentation requests shall be delivered as Technical Reports (CDRL A002).

3.5 INFRASTRUCTURE IMPLEMENTATION SUPPORT

3.5.1 Network Protection System Integration

The contractor shall apply a systems design approach to the directed efforts to ensure that the mission, objectives, and criteria requirements of specified systems are fulfilled. Emphasis shall be on the demonstration of clear, definable and auditable duplication of performance, logistics supportability, reliability and maintainability of the item, subsystems, and systems. The contractor shall also provide demonstration that system designs include consideration for future scalability and adaptability of the item, subsystems, and systems. Preliminary assessments, interim assessments, final assessments, recommendations, and reports shall be delivered as a written Technical Report (CDRL A002). The contractor shall:

- Perform studies, analyze system and/or equipment performance and submit recommendations for development, upgrades, modifications, or alterations of hardware and/or software as appropriate to improve system operation and enhance security posture in the field environment.
- Perform site surveys and deliver survey reports to support the installation of Network Infrastructure, Application and Security Systems.
- Recreate, scientifically within a laboratory environment, an operational environment for local evaluation of field needs. This “modeled” environment may then be manipulated to determine improvements in security posture.
- Perform pre-install population, configuration, and testing of systems.
- Provide onsite engineering support for the installation and upgrade of Network Infrastructure, Application and Security Systems.

- Perform system operation verification test (SOVT) for installed and upgraded systems.

3.6 NETWORK SECURITY OPERATIONS SUPPORT

3.6.1 Network Operations Center Support

The contractor shall work in support of a NIWC Atlantic established network operations center. This network operations center will support the security and network components of the MHS Intranet/MEDCOI. In support of the network operations center, the contractor shall:

- Investigate and troubleshoot network and security components of the MHS Intranet/MEDCOI infrastructure.
- Use the designated configuration management system for the MHS Intranet/MEDCOI to make all approved configuration changes to MHS Intranet/MEDCOI network and security components.
- Provide expertise in configuring, maintaining, upgrading and troubleshooting Cisco switches, routers and firewalls, Juniper routers and firewalls, Palo Alto firewalls, F5 load balancers, InfoBlox DNS appliances, Fidelis XPS security appliances, Citrix NetScaler products, McAfee and SourceFire Intrusion Detection and Prevention products.
- Provide shift work support to enable 24x7 support of the network and security components of the MHS Intranet/MEDCOI.
- Provide expertise in configuration, key loading, troubleshooting and maintenance of tactical encryption devices to include TACLANE and FASTLANE devices.
- Work with manufacturer Tier 3 support to resolve trouble tickets.
- Document all work performed in support of trouble tickets using the approved MHS trouble ticketing system.

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

The contractor shall adhere to the following requirements when the IT support services and/or supply are applicable to the requirement:

- 4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.
- 4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.
- 4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where

available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3C and DoDI 8510.01 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-Department of Navy (DoN).

4.1.7 Ensure all IT products and services recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, Title 36 Code of Federal Regulations Part 1194 – Electronic and Information Technology Accessibility Standards unless otherwise exempt in accordance with the latest regulation.

4.1.8 Only perform work specified within the limitations of the basic contract and task order.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services that support Navy or DoD programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA), contractors that are authorized to use Government supply sources per FAR Subpart 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program as prescribed in DFARS Subpart 208.74 and Government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. The contractor shall purchase the following software and/or software license(s):

Item #	Description	Unit/Issue	Quantity
1	Cisco Meeting Server (CMS) License Renewals (BY)	Ea	3
2	Cisco Meeting Server (CMS) License Renewals (OY1)	Ea	1
3	Cisco Meeting Server (CMS) License Renewals (OY2)	Ea	3

4	Cisco Meeting Server (CMS) License Renewals (OY3)	Ea	1
5	Cisco Meeting Server (CMS) License Renewals (OY4)	Ea	3

4.2.2 DoN Application and Database Management System

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. The RDT&E network does not provide continuous support to operational entities. The contractor shall ensure that any system achieving operation fleet readiness and support is removed from the RDT&E environment and hosted on the respective enterprise solution as required. The contractor shall ensure any systems or applications integrated, installed, or operated on the RDT&E network must be in accordance with DADMS and/or DITPR-DON registration policies. Exemptions to this policy can apply as specified by higher directives. Exemptions on systems that remain on the RDT&E are normally systems that support the RDT&E or have to be on the RDT&E to achieve their target of support.

4.2.3 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact cybersecurity or IA shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate NIAP-approved Protection Profile (PP) for the network involved, and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

4.2.4 Supply Chain Risk Management

“Covered item of supply” (e.g., software, processor, etc.) is any information technology item that is purchased for inclusion in a “covered system” (i.e., national security systems). In accordance with DFARS 252.239-7018, the contractor shall have mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk can be introduced through those components, and shall have implemented or plans to implement countermeasures to mitigate the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

4.3 CYBERSECURITY SUPPORT

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DoN/Navy cybersecurity requirements.

4.3.1 Cyber IT and Cybersecurity Personnel

4.3.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.3.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request – Navy (SAAR-N) form as documented in Para 8.2.2.4(b).

4.3.1.3 Contractor personnel with privileged access shall have a favorably adjudicated Tier 5 background investigation and acknowledge special responsibilities with a Privileged Access Agreement (PAA) in accordance with SECNAVINST 5239.20A.

4.3.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DoN/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DoN Chief Information Officer (CIO) Memorandum: Acceptable Use of DoN IT dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DADMS and is FAM approved can be used as documented in Para 4.2.2. Procurement and installation of software governed by DoN ELAs – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DoN CIO Policy and DoN ELAs awarded.

4.3.3 Cybersecurity Workforce Report

In accordance with DFARS 252.239-7001 and DoD 8570.01-M, the contractor shall identify cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL A003) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in CDRL A003 Attachment 1 of Exhibit A, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. Contractor shall verify with the COR or other Government representative the proper labor category CSWF designation and certification requirements. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the NIWC Atlantic Information Systems Security Manager (ISSM).

4.3.4 Cybersecurity Workforce Designation

CSWF contractor personnel shall perform cybersecurity functions. In accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the CSWF is comprised of the following categories: IA Technical (IAT) and IA Management (IAM); and specialties: Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). Based on the IA function provided by the individual, an IA designator is assigned that references an IA

category or specialty.

Contractor shall have the following quantity of CSWF personnel meeting IA Designator and Level/Position requirements:

IA Designator & Level/Position	Quantity Personnel
IAT II	(70)
CND-IS	(70)
IASAE II	(25)

The following tasks require compliance with the CSWF program and individuals working on those tasks shall be certified at the following baseline levels. All task sections not listed have no CSWF requirements:

PWS Section	IA Designation	CyberSecurity Designation
3.4	None	IASAE-II
3.5	IAT-2	CND Infrastructure Support
3.6	IAT-2	CND Infrastructure Support

5.0 TASK ORDER ADMINISTRATION

Administration of the work being performed is required; it provides the Government a means for task order management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the PM who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

5.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various

times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particular during urgent requirements.

5.2.1 Task Order Status Report

The contractor shall develop a Task Order Status Report (TOSR) (CDRL A004) and submit it monthly; the initial report is due at least 30 days after task order award and on the 10th of each month for those months the task order is active. The prime contractor shall be responsible for collecting, integrating, and reporting any subcontractor reports. This CDRL includes the completion of applicable attachment(s) as cited in the DD Form 1423. The contractor shall deliver the TOSR in an editable format; see applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.2 Closeout Report

The contractor shall develop a task order closeout report (CDRL A005) and submit it no later than 15 days before the task order completion date to allow for any corrective actions. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontracting information, if applicable. See corresponding DD Form 1423 for additional reporting details and distribution instructions. The contractor shall ensure with the COR no corrective action is identified, and if corrective action is necessary, the contractor shall rectify issue prior to the end of task order performance period.

5.2.3 WAWF/PIEE Invoicing Notification and Support Documentation

Pursuant to DFARS 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Wide Area Work Flow (WAWF) application (part of the Procurement Integrated Enterprise Environment (PIEE) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. The contractor shall provide e-mail notification to the COR when payment requests are submitted to the WAWF/PIEE and the contractor shall include cost back-up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in WAWF/PIEE. When requested by the COR, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL A006) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.2.4 Limitation on Subcontracting

Limitation on subcontracting is applicable for task orders that have been wholly or partially set aside for small business or 8(a) concerns above the simplified acquisition threshold. To ensure compliance with the applicable FAR Limitation on Subcontracting requirements, the contractor shall develop and submit a Limitation on Subcontracting Report (LSR) (CDRL A008) every 3 months. See applicable DD Form 1423 for reporting details and distribution instructions. The Government reserves the right to perform spot checks and/or request copies of any supporting documentation.

5.2.5 Electronic Cost Reporting and Financial Tracking (eCRAFT)

The contractor shall complete an Electronic Cost Reporting and Financial Tracking (eCRAFT) Report (CDRL A007) and submit the report on the day and for the same timeframe as when the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. The amounts reported in eCRAFT Periodic Reporting Utility (EPRU) spreadsheet shall be the same reported in WAWF. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination. See applicable task order Attachment eCRAFT Crosswalk and DD Form 1423 for reporting details and upload instructions.

5.3 CONTRACT PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order Quality Assurance Surveillance Plan (QASP). The ability of a contractor to perform to the outlined standards and requirement will be captured in the CPARS. In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Milestones Schedule Plan (CDRL A009) submitted 10 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL A010) submitted monthly.

5.4 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require EVM implementation due to the majority of efforts on this task order is non-scheduled based (i.e., level of effort) and does not lend itself to meaningful EVM information. In lieu of an EVM system, the contractor shall develop and maintain a Contract Funds Status Report (CDRL A012) to help track cost expenditures against performance.

6.0 DOCUMENTATION AND DELIVERABLES

6.1 CONTRACT DATA REQUIREMENTS LIST

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under this task order. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs. The contractor shall not develop any CDRL classified TOP SECRET with Sensitive Compartmented Information (SCI).

Unless otherwise specified, dates are calendar days; one week equals 7 calendar days; 1 days equals 24 hours; and a 24-hour time period is consecutive hours that is exclusive of non-workweek days.

6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL #	Deliverable Title	PWS Reference Para	Frequency	Date Due	Security Classification
A003	CSWF Report	4.3.3, 8.1.2, 8.2.3.1	MTHLY	30 Days after task order award	Unclassified

CDRL #	Deliverable Title	PWS Reference Para	Frequency	Date Due	Security Classification
				(DATO) and monthly on the 10 th	
A004	TOSR	5.2.1, 8.1.2, 8.2.3.1	MTHLY	30 DATO and monthly on the 10 th	Unclassified
A005	Closeout Report	5.2.2, 8.2.2.3	1TIME	NLT 15 days before completion date	Unclassified
A006	Invoice Support Documentation	5.2.3	ASREQ	Within 24 hrs from request	Unclassified
A007	Electronic Cost Reporting and Financial Tracking (eCRAFT) Report	5.2.5	ASREQ	Same date when invoice is submitted into WAWF	Unclassified
A008	Limitation on Subcontracting Report	5.2.6	QRTLY	NLT 105 DATO and every third month on the 10 th	Unclassified
A009	Cost and Milestones Schedule Plan	5.3	One time with revisions (ONE/R)	NLT 10 DATO; revision NLT 7 days after receipt of Govt review	Unclassified
A010	Contractor CDAD Report	5.3	MTHLY	30 DATO and monthly on the 10 th	Unclassified
A011	OCONUS Deployment Package	11.2.1	ASREQ	NLT 30 days prior to travel	Unclassified

6.1.2 Technical CDRL

The following table lists all required technical data deliverables, (CDRLs), applicable to this task order:

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
A001	Program Management Reports, General	3.2.1 – 3.2.4	ASREQ	Within 5 business days of request	Unclassified
A002	Technical/Analysis Reports, General	3.3.1, 3.3.2, 3.4.1, 3.4.2, 3.4.3, 3.5.1	ASREQ	Within 5 business days of request	Unclassified
A012	Contract Funds Status Report (CFSR)	5.4	MTHLY	10 th of Each Month	Unclassified

6.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with NIWC Atlantic corporate standard software configuration as specified below. Contractor shall conform to NIWC Atlantic corporate standards within 30 days of task order award. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	Software to be used
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher/FrameMaker
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	Scheduling	Microsoft Project
f.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio

6.3 INFORMATION SYSTEM COMMUNICATION

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours. The contractor shall have an information system capable of meeting all security requirements identified under Para 8.4.

7.0 QUALITY

7.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality system that meets contract and task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have an adequately documented quality system which contains processes, procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system, which includes an internal auditing system. The contractor shall make their quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this task order may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan or quality system, and development of quality related documents. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- (i) Establish documented, capable, and repeatable processes
- (ii) Track issues and associated changes needed
- (iii) Monitor and control critical process, product, and service variations
- (iv) Establish mechanisms for feedback of field product and service performance
- (v) Implement and effective root-cause analysis and corrective action system
- (vi) Establish methods and procedures and create data used for continuous process improvement

7.2 MANAGE QUALITY COMPLIANCE

7.2.1 General

The contractor shall have quality processes or a Quality Management System (QMS) processes in place that coincide with the Government's Manage Quality processes which address Quality Control, Quality Assurance, Software Quality, and/or project Quality System tasks. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288:2015 for System life cycle processes and ISO/IEC 12207:2017 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in Acquisition Milestones, Phases, and Decision Points, which are standard elements of the Defense Acquisition System and support DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment and objective evidence of Lean Six Sigma, Risk Management, and System Engineering methodologies; and System and Software Engineering best practices.

7.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor's Quality Assurance Plan (QAP) or by the respective Work Breakdown Structure (WBS), Plan of Action & Milestones (POA&M), or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

-

7.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation. The contractor shall have the following related quality objective evidence available for Government review:

- (i) Detailed incoming receipt inspection records
- (ii) First article inspection records
- (iii) Certificates of Conformance
- (iv) Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)
- (v) Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DD Form 254, the contractor shall perform classified work under this task order. At time of task order award, the contractor shall have a TOP SECRET facility clearance (FCL) with SCI access.

8.1.1.1 U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and work within restricted areas unescorted. Access to SCI is limited to U.S. Government Facilities or other U.S. Government sponsored controlled space as authorized on the DD254. The contractor shall not generate any SCI deliverables.

8.1.1.2 This task order requires for various levels of vetting to support specific PWS tasks. The following table outlines the minimum required security clearance per task. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) for access to support the PWS tasks listed below:

Required Security Clearance	PWS Task Paragraph
Top Secret/SCI	3.4.1, 3.6
Secret	3.3, 3.4.2, 3.4.3, 3.5
None required	3.2

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or

access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically a key management person who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government Common Access Card (CAC) and NIWC Atlantic badges (issuances and expiration dates) and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the task order status report (TOSR) (CDRL A004), including updating and tracking data in the CSWF Report (CDRL A003). The FSO shall ensure the latest NIWC Atlantic Contractor Check-in and Check-out (CICO) procedures are implemented and followed.

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30C, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order and are certified/credentialed for the CSWF. A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or NIWC Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum security requirements, the contractor shall permanently remove the individual from NIWC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied," receives an "Interim Declination," or unfavorable fingerprint, the contractor shall remove the individual from NIWC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task orders.

8.2.1 Personnel Clearance

The majority of personnel associated with this task order shall possess a SECRET personnel security clearance (PCL) for access. On a case-by case basis, Top Secret (TS) clearances are eligible for access to Sensitive Compartmented Information (SCI). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD CAF and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and NIWC Atlantic security regulations. The contractor shall immediately report any security incident or insider threat indicator to the NIWC Atlantic Security Management Office, the COR, and Government Project Manager.

8.2.1.1 The following labor categories do not required a minimum personnel clearance (PCL):

Labor Category	Required Minimum Personnel Security Clearance (PCL)	TS/SCI Access required (Y/N)
Administrative Assistant	None required	N

For TS/SCI PCL requirements by tasking, see para 8.1.1.2.

8.2.2 Access Control of Contractor Personnel

-

The contractor shall facilitate the required access for each employee. The ability of the contractor to manage and maintain accessibility in accordance with the applicable requirements is captured in the annual Government CPARS rating.

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities/installations require a CAC for access. Contractor personnel shall carry proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement for any liability issues. For admission to NIWC Atlantic facilities/installations, all contractor personnel must have the COR or Government sponsor initiate access. For contractor personnel requiring a Confidential, Secret, or TS security clearance, a visitor authorization request (VAR) must be submitted via the Defense Information System for Security (DISS) to the applicable Security Management Office (SMO). For Charleston and other remote locations excluding Tidewater, the contractor shall send VAR to SMO 652366. For access requiring a TS/SCI security clearance, the contractor shall send an additional VAR to Special Security Office (SSO) 652363. If faxing a VAR versus using DISS, the contractor shall submit their request on company or agency letterhead to (843)218-4045 for Charleston or (757)541-5860 for Tidewater locations. For visitation to all other Government locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office.

JPAS is replaced by DISS. The contractor shall ensure they are capable of accessing DISS when JPAS is no longer accessible. After DISS transition date, contractor shall submit all VARs through DISS.

(b) Contractor employees who make repeated deliveries to Joint Base (JB) Charleston military installations and do not require access into NIWC Atlantic facilities or access to IS shall obtain a base access card. Only contractor employees that are able to obtain a card will be eligible for entrance on base. At JB Charleston, the contractor shall obtain the required access card via the Defense Biometric Identification System (DBIDS) from the JB Charleston Badge and Pass Office. Contractors with employees that are no longer employed shall return the employee's access card directly to the COR or to the local NIWC Atlantic Security Office with COR notification within five (5) days from the last day of employment. Contractors who do not have a DBIDS card or CAC will receive a one-day pass for each day access is required. Information about DBIDS is found at <https://dbids-global.dmdc.mil/enroll#!/>.

(c) All contractor persons engaged in work while at a Government facility/installation shall be subject to inspection of their

vehicles, identification cards, and bags/parcels at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

(d) The contractor shall notify the COR and appropriate NIWC security personnel within 24 hours from the time contractor employee gives notice of departure or are removed unexpectedly from contract support. For contractors in direct support of NIWC Atlantic, see the Contractor Check-in and Check-out (CICO) Procedures requirements listed in Para 8.2.2.5.

8.2.2.2 Identification and Disclosure Requirements

All contractor and subcontractor employees located on and off Government installations shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement:

(a) Contractor employees shall be clearly identifiable as a contractor while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors shall identify themselves as contractors or subcontractors during meetings, on attendance meeting list/minutes, at the beginning of telephone conversations, in electronic messages including their electronic digital signature, and all correspondence related to this task order.

(c) Contractors occupying facilities within Department of the Navy or other Government installations (such as offices, separate rooms, or cubicles) shall clearly display and identify their space with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

8.2.2.3 Government Badge Requirements

Depending on access required, contractor personnel shall require a Government-issued picture badge. While on Government installations/facilities, contractors shall abide by each site's latest security badge requirements and prominently display (above the waist) their Government-issued picture badge. Government installations/facilities are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards.

(a) Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, etc.) to the applicable Government security office via the COR who will validate the need authorizing contractor performance within the applicable Government installation/facility.

(b) The contractor shall assume full responsibility for the proper use and security of the identification badge and is responsible for returning the badge upon termination of personnel or expiration or completion of the task order.

(c) The contractor (FSO if applicable) shall track all personnel (including subcontractors) holding CAC and/or NIWC Atlantic Government badges in support of this task as part of the TOSR. At the completion of the task order, the contractor shall provide a list as part of the Closeout Report (CDRL A005) of all returned and unreturned badges with a written explanation for any missing badges.

8.2.2.4 Common Access Card Requirements

Contractors supporting work that requires access to Government facilities/installations and/or access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoDM 1000.13-V1, issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD federally controlled facilities on behalf of the NIWC Atlantic on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS).
3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoDM 5200.02 – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. Contractor personnel requiring logical access shall obtain and maintain a favorable T3 investigation. Contractor personnel shall contact the NIWC Atlantic Security Office to obtain the latest CAC requirements and procedures.
4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a PKI. A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed SAAR-N form to the task order specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Atlantic ISSM office:

1. For annual DoD Cybersecurity/IA Awareness training, the contractor shall use this site: <https://mytwms.dc3n.navy.mil/>. For contractors requiring initial training and do not have a CAC, contact the NIWC Atlantic ISSM office at phone number (843)218-6152 or e-mail questions to NIWCLANT.ISSM.OPS.FCT@navy.mil for additional instructions. Training can be taken at the ISSM office or online at <https://public.cyber.mil/training/cyber-awareness-challenge/>.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form and shall initiate a CAC request via the latest Contractor Check-in procedures as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website at <https://www.public.navy.mil/navwar/atlantic/pages/contractorcheckin.aspx>.

8.2.2.5 Contractor Check-in and Check-out (CICO) Procedures

All NIWC Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a NIWC Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out (CICO) procedures, instructions, and forms as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website (under “Contact” tab, select “Contractor Check-In”). In accordance with the monthly status reporting requirements, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the CICO instructions. The contractor (FSO, if applicable) shall have IT access to NIWC Atlantic systems for purposes of meeting CICO personnel requirement. For contractor employees whose services are no longer required, the contractor shall ensure all those employees return all applicable Government credentials (keys, CAC, site badges, tokens, etc.) and any assigned Government-furnished property (e.g., laptops) are returned to the COR or appropriate Government representative. The contractor shall ensure all procedures as cited in the Contractor Check-out COG page are followed which includes a completed Contractor Check-out checklist form (SPAWARSYSCEN 5500/3) is submitted for each employee as applicable.

8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel shall not access the Navy Enterprise Resource Planning (Navy ERP) system.

8.2.3 Mandatory Training

In addition to training requirements and certifications required for a specific labor category, certain contractor personnel (including subcontractors) regardless of security classification shall complete required mandatory training in accordance with NAVWARSYSCOM Code 80330 mandatory training webpage: <https://wiki.spawar.navy.mil/confluence/x/jwDsAQ>. Contractors without access to the training webpage shall coordinate with the COR concerning the latest mandatory training as specified on the training webpage. The following table is a sample of contractor mandatory training that is subject to change in accordance with the NAVWARSYSCOM website or SECNAVINST:

#	Training Course Name	Contractor Personnel Applicability
1	Active Shooter, Level 1	All contractors
2	Operations Security (OPSEC)	All contractors
3	Antiterrorism Training, Level 1	Contractors requiring routine physical access to federally controlled facilities or military installations (DFARS 252.204-7004)
4	[NIWC Atlantic] Annual Security Refresher	All fulltime/partial, onsite contractors
5	Suicide Prevention Training (Suicide Awareness)	All fulltime, onsite contractors
6	Records Management	All contractors NMCI account holders
7	DoD Cyber Awareness Challenge	All contractors NMCI account holders and Personnel accessing CAC-enabled gov't sites – Authorized users of DOD information systems and networks
8	Privacy and Personally Identifiable Information (PII) Awareness Training	All contractors with access to PII
9	NIWC Intelligence Oversight	All contractors

10	Sensitive Compartmented Information (SCI) Initial/Refresher Training	Contractors that are SCI cleared personnel and authorized users of DOD IS and networks
----	--	--

8.2.3.1 The contractor shall be responsible for verifying applicable personnel receive all required training within the specified due dates. The contractor shall track and annotate all mandatory training required and completed for each employee in the Staffing Plan which is part of the monthly TOSR (CDRL A004). For CSWF, contractor shall ensure all mandatory cybersecurity training and certifications are reported in the CSWF Report (CDRL A003).

8.2.3.2 Unless otherwise noted, the contractor shall complete mandatory training annually between 1 October and 30 September utilizing the Total Workforce Management System (TWMS). For some personnel, attendance of Government face-to-face training is allowed if COR concurs with training schedule. For training taken via Defense Information Systems Agency / Navy Knowledge Online (DISA/NKO), the contractor shall forward a copy of the certificate to ssclant_mandatory_tr.fcm@navy.mil who will upload or ensure each completed training is recorded in TWMS.

8.2.4 Accessing Government Information Systems and Nonpublic Information

Contractor personnel shall meet the following cybersecurity and personnel security requirements when accessing Government information systems and nonpublic information.

Definition – For the purposes of this section, “sensitive information” includes the following:

- (a) all types and forms of confidential business information, including financial information relating to a contractor’s pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
- (b) source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 2101-2107);
- (c) information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;
- (d) other information designated as sensitive by NIWC Atlantic and the program.

8.2.4.1 In the performance of the contract/order, the contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

8.2.4.2 Contractor personnel shall protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract/order, whether the information comes from the Government or from third parties. The contractor shall provide the following support:

- (a) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract/order, and not for any other purpose unless authorized;

(b) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract/order or as authorized by Federal statute, law, or regulation;

(c) Inform authorized users requiring access in the performance of the contract/order regarding their obligation to utilize information only for the purposes specified in the contract and to safeguard information from unauthorized use and disclosure.

(d) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment.

(e) Notify the Contracting Officer in writing of any violation of the requirements in Para 8.2.4.2(a) through Para 8.2.4.2(d) as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

8.2.4.3 In the event that the contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

8.2.4.4 The requirements of this text are in addition to any existing or subsequent OCI requirements which may also be included in the contract/order, and are in addition to any personnel security or Information Assurance requirements, including SAAR-N form (DD Form 2875), annual Cybersecurity training certificate, Questionnaire for Public Trust form (SF85P), or other forms that may be required for access to Government Information Systems.

8.2.4.5 Subcontracts. The contractor shall insert Para 8.2.4.1 through 8.2.4.4 in all subcontracts that may require access to sensitive information in the performance of the contract/order.

8.2.4.6 Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract/order. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of Para 8.2.4.2 and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract/order from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

8.2.5 Handling of Personally Identifiable Information (PII)

In accordance with the Privacy Act of 1974, the contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of Personally Identifiable Information (PII) in accordance with the latest DoN policies. The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in the header and footer of each page of the document: "CUI". In addition to marking documents at the top and bottom with "CUI" a CUI "Designation Indicator Block" is required at the bottom of the document's first page within the "CUI" banner and footer markings. DoD guidance directs that this block be located at the lower right of the page. Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Once notified, the Contracting Officer shall immediately contact the Privacy Act Coordinator. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. If a contractor, including any subcontractor, is authorized access to PII, the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act.

8.3 OPERATIONS SECURITY REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, NIWC Atlantic's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall develop their own internal OPSEC program specific to the task order and based on NIWC Atlantic OPSEC requirements. At a minimum, the contractor's program shall identify the current NIWC Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial OPSEC training within 30 days of contract/task order award and annual OPSEC awareness training in accordance with requirements outline in the Mandatory Training, Para 8.2.3. OPSEC training requirements are applicable for personnel during their entire term supporting this NIWC Atlantic task order.

8.3.3 NIWC Atlantic OPSEC Program

Contractor shall participate in NIWC Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract/order shall have specific OPSEC requirements listed on the DD

Form 254.

8.4 INFORMATION SYSTEM SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

8.4.1 Hardware and Software

The contractor shall scan all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure Data-at-Rest encryption technology is installed on all portable electronic devices including storage of all types.

8.4.2 Safeguards

The contractor shall protect Government information and shall be able to provide documentation (e.g., Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252.204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

8.4.2.3 Sanitize media (e.g., overwrite, reformat, or degauss) before external release or disposal.

8.4.2.4 Encrypt all information that has been identified as CUI when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DoD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

8.4.2.5 Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

8.4.2.6 Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption. The contractor shall encrypt or digitally sign all communications for authentication and non-repudiation.

8.4.2.7 Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

8.4.2.8 Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

8.4.2.9 Provide protection against computer network intrusions and data exfiltration, minimally including the following:

(a) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(b) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(c) Prompt application of security-relevant software patches, service packs, and hot fixes.

8.4.2.10 As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

8.4.2.11 Report loss or unauthorized disclosure of information in accordance with contract, task order, or agreement requirements and mechanisms.

8.4.2.12 Pursuant to DFARS 252.204-7009, the contractor shall not use or disclose third-party contractor reported cyber

incident information. The contractor can be held liable for breach of information and shall extend restriction in subcontracts for service that include support to Government's activities related to safeguarding covered defense information and cyber incident reporting.

8.4.2.13 As applicable, follow minimum standard in SECNAVINST 5510.36B for classifying, safeguarding, transmitting, and destroying classified information and CUI.

8.4.3 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.4.4 Covered Defense Information

The contractor shall identify all covered defense information, as defined in DFARS 252.204-7012, and apply markings when appropriate to all deliverables in accordance with DoDI 5200.48.

8.4.5 Utilization of Contractor Furnished Government-controlled Equipment

For the purposes of this contract/order, contractor-owned computer assets loaded with a secure government furnished computing image will be known as Government Controlled Equipment (GCE). The contractor shall meet specific operational requirements when utilizing a Contractor furnished laptop with a Government-controlled software image (refer to section 9.0).

At a minimum, contractor personnel shall comply with the following requirements when utilizing a Contractor issued Government-controlled computer asset:

8.4.5.1 Contractor personnel shall arrange with the appropriate Government personnel for contractor-owned computer assets to be loaded with appropriate Government software platform images.

8.4.5.2 All messages sent to/from utilize virtual private network (VPN) connections.

8.4.5.3 All messages sent to/from are encrypted.

8.4.5.4 No storage of data on non-compliant networks (e.g., contractor's corporate systems).

8.4.5.5 Only government email (NMCI, mail.mil, etc.) is allowed to be used; absolutely NO Gmail, other personal systems, and NO corporate email that does not reside on NIST compliant systems shall be utilized.

8.4.5.6 All email must be sent between compliant systems – e.g., sending encrypted email to a private corporate account that resides on an uncompliant network, then decrypting and utilizing it is not allowed.

8.4.5.7 All stored information meets data-at-rest encryption standards – if using GFP, then use the same methods as networked devices (e.g., MS Bitlocker, Symantec Endpoint Security, etc.)

8.4.5.8 All data is housed on GFE shared storage location – ensures government can retrieve its data at any time.

8.4.5.9 In regard to processing, storing or transmitting CUI, no CUI is allowed on an information system not meeting configuration and security standards.

8.5 ENHANCED SECURITY CONTROLS

The contractor shall not process, store, or transmit controlled unclassified information (CUI), as defined in DoDI 5200.48, on any information system and IT asset that is owned, or operated by or for, the contractor except for computer assets identified as Government controlled equipment (GCE).

9.0 GOVERNMENT FURNISHED INFORMATION

For the purposes of this task order, Government Furnished Information (GFI) includes manuals, technical specifications, software, software licenses, maps, building designs, schedules, drawings, test data, etc. provided to contractors for performance on this task order. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution. . The Government will mark any CUI which includes unclassified covered defense information and unclassified controlled technical information provided to the contractor. For any missing markings, contractor shall request appropriate marking from the Government.

GFI is utilized on this task order. Any applicable document (PWS Para 16.0) not available online, the Government will provide document as GFI listed in the table below. The contractor shall inventory all GFI by tracking distribution and location and provide a GFI inventory to the Government. The contractor shall use the GFI provided to support this task order only – use of GFI document(s) to support other projects beyond this task order is not allowed. Unless otherwise specified, all GFI will be provided by the Government by the estimated delivery date listed in the table below, and the contractor shall return all GFI to the Government at completion of the task order. If a contractor requires additional GFI other than what is listed, the contractor shall submit a request to the COR within 30 days after task order award.

The contractor shall utilize Government-provided and Government-controlled software platform images on all contractor-owned computer assets supporting Section 3.0 of this contract/task order. The contractor shall maintain ownership of the computing hardware and as such shall maintain the hardware platform to include replacement of the platform due to equipment breakage or malfunction. The contractor shall also provide upgraded hardware as necessary to support upgrades to the government furnished computing image as required. At the end of the contract, or during performance where GCE is removed from service or replaced by the contractor, the contractor shall make arrangements for the government to remove the secure computing image and government data from all contractor owned computing hardware before it is returned to the contractor for their final disposition.

Item #	Description	GFI Estimated Delivery Date
1	Microsoft Windows computing platform image	14 days after task order award

10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes GFP and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

-

GFP will not be provided and CAP is not anticipated on this task order.

-

The contractor shall furnish X-86 compatible computing platforms as an indirect cost for each employee executing tasking under section 3.0 that is capable of exclusively running the secure software image furnished under section 9.0. The contractor shall enable the government to install this software image on the computing hardware and allow the government to subsequently maintain the secure software image such that the computing hardware running it can be classified as Government Controlled Equipment (GCE).

The contractor shall maintain ownership of the computing hardware on the contractor furnished laptops and as such shall maintain the hardware platform to include replacement of the platform due to equipment breakage or malfunction. The contractor shall also provide upgraded hardware on the contractor furnished laptops as necessary to support upgrades to the government furnished computing image as required. At the end of the contract, or during performance where GCE is removed from service or replaced by the contractor, the contractor shall make arrangements for the government to remove the secure computing image and government data from all contractor owned computing hardware before it is returned to the contractor for their final disposition.

11.0 TRAVEL

11.1 LOCATIONS

(b) (4)

The contractor shall be prepared to travel to all the locations cited in Attachment #4. Contractor personnel traveling in support of DoD shall travel in accordance with the latest Joint Travel Regulations (JTR) at time travel is being performed. The contractor shall comply with travel cost pursuant to FAR 31.205-46. The contractor shall notify the COR prior to traveling to

ensure Government coordination.

Exact travel dates are not known at time of task order award, and locations are subject to change. The proposed travel locations identified are based on historical data. The contractor shall be able to travel to any of the sites noted in Attachment 3.

Travel outside of the continental United States (OCONUS) which includes Alaska, Hawaii, and all foreign countries is required. The applicable countries are included in the Attachment 3. Prior to travel, the contractor shall meet all necessary travel requirements for their company and personnel to support work in the noted foreign OCONUS sites.

11.2 OCONUS TRAVEL REQUIREMENTS

Pursuant to SPAWARSYSCENLANTINST 12910.1B, DoDD 4500.54E, and the latest DoD Foreign Clearance Guide requirements, the contractor shall travel to Outside Contiguous United States (OCONUS) sites to support deployed forces. The contractor shall be familiar with and able to obtain approvals in the Aircraft and Personnel Automated Clearance System (APACS) as well as submitting and requesting letter of authorization (LOA) in the web-based Synchronized Pre-deployment & Operational Tracker (SPOT).

11.3.1 General OCONUS Requirements

The contractor shall ensure compliance with applicable clauses and travel guide requirements (including completion of any mandatory training) prior to traveling to each of the specified travel locations. The contractor shall be responsible for knowing and understanding all travel requirements as identified by the applicable combatant command (CCMD) and country. The contractor shall be responsible for submitting applicable deployment forms and/or deployment packages (CDRL A011) to the COR or task order technical POC and NIWC Atlantic Deployment Manager no later than 30 days prior to travel. For all OCONUS travel, the contractor shall submit an official OCONUS Travel Form (NIWCLANT 12990/12) and shall ensure all OCONUS travel has an approved Aircraft and Personnel Automated Clearance System (APACS) request. The COR will provide a blank travel form after task order award.

11.3.2 OCONUS Immunization Requirements

Pursuant to DoDI 6205.4, SPAWARSYSCENLANTINST 12910.1B, and any additional DON specific requirements, contractor employees who deploy to OCONUS locations both shore and afloat shall require up to date immunizations. The contractor shall review and verify if their personnel meet any immunization requirements prior to assigning personnel to travel.

11.2.3 Emergency Medical Screening for OCONUS Travel

During emergency related situations including health (e.g., COVID-19 pandemic) and weather related circumstances, contractor personnel shall perform official OCONUS travel in accordance with the latest directions outlined in the NIWC Atlantic COG, related DoD travel websites, and the Centers for Disease Control and Prevention (CDC) website. To the extent possible, contractor personnel shall follow the same travel regulations and restrictions as Government civilian personnel. When in doubt concerning applicability, the contractor shall verify requirements with COR and NIWC Atlantic OCONUS Travel Team. Depending on the latest travel regulations which may differ based on location, contractor personnel shall be prepared to meet additional requirements such as medical testing prior to travel. These requirements will be identified by the COR. Contractor personnel shall complete any required health screening/testing and complete screening questionnaire which shall all be submitted to the COR prior to travel.

11.2.4 Letter of Authorization

The contractor shall have a LOA signed by the designated Contracting Officer for any and all OCONUS Travel. An OCONUS Travel Form (NIWCLANT 12990/12) is required for all travel locations OCONUS to include Alaska, Guam, Hawaii, Kwajalein Atoll, Johnston Atoll, Midway Islands/Atoll, Puerto Rico, US Virgin Islands, Wake Island, etc. If the travel location is not in "the lower 48"/CONUS, then an OCONUS Travel Form is required prior to the LOA being Government Authorized by an employee of the NIWC Atlantic OCONUS Travel Team in order for the Contracting Officer to approve. The LOA identifies any additional authorizations, privileges, or Government support that contractor personnel are entitled to under contract and task order, if applicable. The contractor shall initiate a LOA for each prospective traveler. The contractor shall use SPOT or its successor, at <https://spot.dmdc.mil/privacy.aspx>, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed and approved by the SPOT registered Contracting Officer of this task order. Contractor personnel traveling in support of NIWC Atlantic shall travel with a hardcopy approved LOA in their possession

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the task orders. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

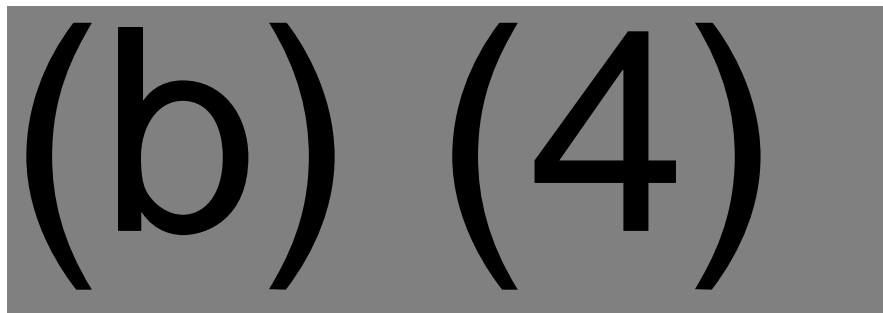
13.0 SUBCONTRACTING REQUIREMENTS

If the prime contractor is planning to utilize subcontractor(s) on this task order, the prime contractor shall identify the applicable subcontractor(s) in its proposal for the task order. Should the prime contractor be awarded a task order, only those subcontractors included in the proposal upon which the award is based are approved for use on the task order. Post award subcontractor additions (i.e. subcontractor additions to a task order after issuance of the order) are governed by FAR 52.244-2.

In addition, while Government consent to subcontract is not required for prime contractors with an approved purchasing system, if after award of a task order the prime contractor intends to enter into a subcontract with an entity not identified in its proposal upon which the task order award was based, the prime contractor shall nevertheless notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the task order. Such notification shall include, (i) a description of the supplies or services to be subcontracted, (ii) identification of the subcontract type to be used, (iii) identification of the proposed subcontractor, and (iv) the proposed subcontract price.

13.1 AUTHORIZED SUBCONTRACTORS

The following subcontractor(s) is either identified by the contractor at the time of award of the task order, have been consented to by the Government pursuant to the Subcontracts clause of the contract, or, in the event the contractor has an approved purchasing system, the contractor has provided notification in accordance with paragraph 13.0 above:



14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment 2.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 ON CALL SUPPORT

The contractor shall provide a method for 24x7 voice and email communication with the Government.

15.2 WORKWEEK

All or a portion of the effort under this task order will be performed on a Government installation. The contractor shall provide support services corresponding to Government workweek and core hours. Normal workweek is Monday through Friday. Pursuant to Federal law (5 U.S.C. 6103), the Government observes the following public holidays per year. For planning purposes, contractors working in Government spaces shall treat these holidays as Government non-work days which may affect accessibility to Government space.

Name of Holiday	Time of Observance
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May

Juneteenth	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday will be observed by the Government on the prior Friday or following Monday, respectively.

15.3 EXTENDED WORK WEEK

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week (EWW) may be required for professional (i.e., salaried) employees.

15.4 OVERTIME FOR SCLS LABOR CATEGORIES

Work will be performed during normal working hours when practical. Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, overtime (OT) will be allowed for Service Contract Labor Standards (SCLS) labor categories in accordance with FAR 52.222-2. This task order does not allow for payment of overtime during the normal workweek for employees who are exempt from the Fair Labor Standards Act unless expressly authorized by the Contracting Officer. Under Federal regulations, the payment of overtime is required only when a non-exempt employee works more than 40 hours in a normal week period. Prior to working OT hours, the contractor shall obtain COR concurrence for the specific hours per labor category and applicable dates.

15.5 FUNDING ALLOCATION

This task order is funded with multiple appropriations with various Accounting Classification Reference Numbers (ACRNs) which may or may not cross multiple contract performance years. Depending on the services performed and the applicable timeframe, the contractor shall invoice cost in accordance with Section B, Section C, and Section G of the task order award. Unless otherwise advised, the contractor shall itemize all summary of work and financial information in the TOSR CDRL by each CLIN. The ability of the contractor to perform adequate billing and accounting will be reflected in the contractor's annual Government CPARS rating.

15.6 TRANSITIONAL PLAN

To minimize loss in productivity and to mitigate negative impact to on-going support services when new contractors are introduced,

the contractor shall provide support during the transition-in and transition-out periods. The contractor shall have personnel on board within the first sixty days after award. Note: this time period is part of funded task order transitional periods at the beginning and end of the task order. After task order award (transition-in), the contractor shall work with the exiting contractor and become familiar with performance requirements in order to commence full performance of services before the out-going contractor leaves the site. Prior to the completion of the task order (transition-out), the contractor shall work with any new contractor personnel to ensure continuous support between contracts.

16.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise indicated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever practical.

16.1 REQUIRED DOCUMENTS

The contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	Title
a.	DoDM 5200.01	DoD Manual – Information Security Program (vol 1, 2, 3) dtd 24 Feb 12 with Change 2/4/3 dtd 28 Jul 20
b.	DoDM 5200.02	DoD Manual – Procedures for the DoD Personnel Security Program dtd 3 Apr 17
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12 with Change 2 dtd 20 Aug 20
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08 with Change 1 dtd 26 Apr 18
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06 with Change 2 dtd 18 May 16
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program (NISP) dtd 18 Mar 11 with Change 2 dtd 24 Sep 20
g.	DoDI 5200.48	DoD Instruction - Controlled Unclassified Information (CUI) dtd 6 Mar 20
h.	DoDI 6205.4	DoD Instruction – Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
i.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 05 Oct 20
j.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14 with Change 1 dtd 07 Oct 19

	Document Number	Title
k.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14 with Change 2 dtd 28 Jul 17
l.	DoD 8570.01-M	DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent replacement)
m.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16
n.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd June 2016 (and subsequent revisions)
o.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DoN Cyberspace IT and Cybersecurity Workforce Management and Qualification dtd 10 Feb 16
p.	SECNAVINST 5510.30C	Secretary of the Navy Instruction – DoN Personnel Security Program (PSP) Instruction dtd 6 Oct 06
q.	SPAWARINST 3432.1	Space and Naval Warfare Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
r.	SPAWARSYSCENLANTINST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
s.	SPAWARSYSCENLANTINST 12910.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Government and Contractor Personnel Outside the Continental Unlisted States dtd 23 Aug 16
t.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
u.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a

16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title
a.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
b.	DoDM 1000.13-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14
c.	DoDD 5000.01	DoD Directive – The Defense Acquisition System dtd 20 Nov 07
d.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System dtd 7 Jan 15
e.	ISO/IEC/IEEE 12207:2017	International Organization for Standardization/ International Electrotechnical Commission/Institute of Electrical and Electronics Engineers: Systems and Software Engineering –

	Document Number	Title
		Software Life Cycle Processes
f.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04
g.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
j.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
k.	N/A	NIWC Atlantic Public website – CICO Procedures https://www.public.navy.mil/navwar/atlantic/pages/contractorcheckin.aspx
l.	N/A	NAVWARSYSCOM Code 80330 mandatory training webpage – https://wiki.spawar.navy.mil/confluence/x/jwDsAQ
m.	N/A	DoD Foreign Clearance Guide – https://www.fcg.pentagon.mil/fcg.cfm

16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

END OF PWS